APPENDIX C

GUIDELINES FOR COMMAND SECURITY INSTRUCTION

1. A written command security instruction or written procedures are necessary to ensure the security requirements contained herein are established for local command operations. In composing a command security instruction or procedures, the security manager must consider whether a function will be required frequently enough to warrant detailed instruction. Consider the size, mission, and scope of the command's authority when selecting topics for instructional elaboration. There is no need to duplicate the requirements contained in this instruction, rather the procedures should supplement the Department of the Navy Information and Personnel Security Program Regulations, and other directives. The guidelines that follow may be helpful in developing the personnel security program portions of your command security instruction.

a. The introduction to the command security instruction should cover the purpose of the instruction, its applicability to all in the command and its relationship to other directives.

b. The majority of the command instruction will concentrate on the command's internal administrative procedures leading to access to classified information or assignment to sensitive duties for command personnel as well as procedures for safeguarding and maintaining classified information. The text will:

(1) Explain each requirement step by step, specifying responsible entities as necessary (eg. if your command is serviced by a centralized personnel office, it will be necessary to spell out the division of personnel security responsibilities between the command security and personnel entities and the centralized personnel office).

(2) Identify the command's security organization, chain of command, including specific areas of responsibility. Elaborate on any requirements peculiar to the command. Indicate organizational relationships and cite any security servicing agreements. Describe procedures for internal security reviews and inspections (including subordinate inspections if appropriate).

(3) Include a security education program using guidelines in chapter 4 of this instruction. Identify personnel responsible for the security education program including specific areas of

responsibility (i.e. briefings and debriefings).

(4) Detail the internal procedures for reporting and investigating compromises and other security violations. Establish channels for reporting counterintelligence matters to the Naval Criminal Investigative Service (NCIS) and procedures for requesting NCIS assistance and identify the NCIS servicing office. If your command has subordinate commands who would be required to forward JAG Manual investigations to you for review, assign responsibilities for review in compromise cases.

(5) Include in this section a list of areas within the command authorized for general visiting and clearly identify all areas that are off-limits to visitors. Assign responsibilities for processing classified visit requests to or from the command.

(6) Formulate guidelines for foreign travel briefings and identify the individual responsible for briefing/debriefing.

(7) If your command hosts foreign exchange personnel/students, or foreign liaison officers, specify any restrictions on movement and caution command personnel regarding their responsibilities.

(8) Assign responsibilities for final preparation of investigative request forms.

(9) Establish procedures for documenting clearance and access granted.

(10) Assign responsibilities for continuous evaluation. Establish procedures for reporting derogatory information to the DON CAF.

(11) Identify the adjudicative guidelines, remind command personnel of their continuing responsibilities to notify security of derogatory information or suspicious behavior.

c. In managing the personnel security program, as with all aspects of security, insure that provisions are in place to monitor the program constantly to assure the procedures are up to date and that they meet the ever changing security needs of your command.

2. Refer to reference (d) for guidance concerning the development of local security requirements for classification management, accounting, control, reproduction, declassification and destruction of classified information.